## BRIEF OVERVIEW OF HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law by President Clinton on August 21, 1996. Title II of the law covers administrative simplification, which is the topic of this paper.

HIPAA must be implemented by any health care entity that creates, stores, or transmits health care data in an electronic format, including public and private entities, healthcare plans and providers, veterans and Indian healthcare programs, employee benefit plans, long-term care, and Medicaid, Medicare, and Medicare supplemental plans.

## ADMINISTRATIVE SIMPLIFICATION

The administrative simplification provisions standardize the electronic transmission of certain administrative and financial transactions, and protect the security and privacy of transmitted information. The four parts of Administrative Simplification, discussed below, are Electronic Health Transactions Standards, Unique Identifiers, Security & Electronic Signature Standards, and Privacy & Confidentiality Standards*. Note that security refers to protecting access to data, while privacy refers to the authorized disclosure of data.*

DSHS has 26 months from the effective date of each final rule to achieve compliance. Only the Transactions and Code Sets standard has a final rule publication date, which is June 30, 2000. For updated information, see DHHS' Schedule for Publication of the regulations at http://aspe.hhs.gov/admnsimp/asmiles.htm

| **Standard** | **NPRM Published** | **Expected Final Rule Publication** | **Expected Date Compl. Reqd** |
|---|---|---|---|
| Transactions and Code Sets | 5/07/1998 | 6/2000 | 8/2002 |
| National Provider Identifier | 5/07/1998 | | |
| National Employer Identifier | 6/16/1998 | | |
| Security | 8/12/1998 | | |
| Privacy | 11/3/1999 | | |
| National Health Plan Identifier | | | |
| Claims Attachments | | | |
| Enforcement | | | |
| National Individual Identifier | On Hold | | |

**Figure 1, Implementation Schedule**

## I. ELECTRONIC HEALTH TRANSACTIONS AND STANDARDS

The term *"Electronic Health Transactions"* includes health plan enrollment, de-enrollment, maintenance, care authorization, referrals, certification, health claims activities including claim status; premium payments, care payments, coordination of benefits, and related transactions.

A listing of electronic HIPAA transactions, including the number of required data elements in parenthesis, includes:

- Pharmacy claims (147)
- Dental health care claims (243)
- Professional health care claims (493)
- Institutional health care claims (525)
- Health care payment and remittance (247)
- Professional claim coordination of benefits (493)
- Institutional claim coordination of benefits (525)
- Dental claim coordination of benefits (243)
- Health claim status report and response (88)
- Benefit enrollment and maintenance (177)
- Health care eligibility inquiry and response (149)
- Payment order/remittance advice (67)
- Health care service review information (203)

The mandatory use of transaction standards applies to all electronic transmissions of healthcare data. A transmission where the data is physically moved from one location to another using magnetic tape, disk, or CD media is included.

Health organizations also must adopt *Standard Code Sets* to be used for all health transactions. For example, coding systems that describe diseases, injuries, and other health problems, as well as their causes, symptoms and actions taken must become uniform. All parties to any transaction will have to use and accept the same coding. HIPAA Transaction Standards via the Implementation Guides define a Master Data Dictionary.

## II. Unique Identifiers For Providers, Employers, Health Plans And Patients

The current system allows the use of multiple ID numbers when dealing with clients, which HIPAA sees as confusing, conducive to error and costly. It is expected that standard identifiers will reduce these problems.

## III. Security Of Health Information & Electronic Signature Standards

The new Security Standard, expected to be approved in August 2000, will provide a uniform level of protection of all health information that is 1) housed or transmitted electronically, and that 2) pertains to an individual. The proposed standard covers administrative procedures, physical safeguards, technical security services, and technical security mechanisms. While each of these areas contain a host of requirements, only the more significant requirements follow.

- Certifying computer systems
- Chain of trust (data sharing) agreements
- Contingency planning/disaster recovery
- Policy covering internal auditing and security training
- Designating and assigning responsibility for security
- Facility security plan that includes visitor and escort controls
- Electronic access controls using one or a combination of context-based, role-based, or user based procedures
- An alarm, audit trail and event reporting capability to become aware of, track, and report unauthorized access attempts.

## IV. PRIVACY AND CONFIDENTIALITY

On November 3, 1999, DHHS published a proposed rule protecting the privacy of information related to an individual's health, treatment or healthcare payment. The rule, which overlays HIPAA's entire Administrative Simplification provision, would:

- Give individuals the right to receive written notice of information practices;
- Give individuals the right to access and amend their health information;
- Require health plans and providers to provide an audit trail of health information disclosures;
- Require health plans and providers to get individuals' written authorization for use of their information for purposes other than treatment, payment or healthcare operations; and
- Require organizations to limit the information disclosed to the minimum amount necessary.

## CONSIDERATIONS FOR IMPLEMENTING HIPAA

How each organization in DSHS implements HIPAA will depend on the type of health care information processed and/or stored by the organization. Following are some common factors to consider:

1. Identify all applications and feeder systems that process or store healthcare information. Identify transaction types and code sets currently in use, and determine HIPAA compliance of current transaction types.

2. Identify business partners, clients, etc. with whom health care data is exchanged. Contact business partners to determine their HIPAA compliance plans. Determine methodology to secure the business partner relationship and involve legal counsel for all contract revisions.

3. Perform a HIPAA impact analysis in order to make educated and strategic decisions regarding which systems require changes, and where a change may impact other systems.

5. Develop a comprehensive action plan, including:

    - Developing new policies, processes, and procedures
    - Building "chain of trust" agreements with business partners
    - Re-designing a compliant technical information infrastructure
    - Purchasing new, or adapting, information systems
    - Training and enforcement

6. Develop a plan with deadlines and timetables. (See Appendix A for DOH plan).

Detailed Implementation Guides are available from the Washington Publishing Company for web download of electronic documents or purchase of bound hardcopy. The URL for The Washington Publishing Company is http://www.wpc-edi.com/hipaa/